

REMARKS

Applicants respectfully request further examination and reconsideration in view of the instant response. Claims 1-5, 7-11, 13-16 and 18-44 remain pending in the case. Claims 1-11 and 13-44 are rejected. Claims 6 and 17 are cancelled herein without prejudice. Claims 1, 16, 18, 25, 30 and 31 are amended herein. No new matter has been added as a result of the amendments. Support for the amendments can be found in the instant specification at least at page 14, lines 2-4, and Figure 4A.

35 U.S.C. §103 - Claims 1-5, 7, 8, 11, 13, 14, 16, 17, 19-22, 30, 36, 37 and 44

The Office Action mailed December 18, 2008, hereinafter referred to as the “instant Office Action,” states that Claims 1-5, 7, 8, 11, 13, 14, 16, 17, 19-22, 30, 36, 37 and 44 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Application Publication No. 2004/0196975 by Zhu et al., hereinafter referred to as “Zhu,” in view of 2002/0174332 by Vialen et al., hereinafter referred to as “Vialen.” Claim 17 is cancelled herein without prejudice; therefore a discussion of the rejection of Claim 17 is moot at this time. Applicants have reviewed Zhu and Vialen and respectfully submit that the embodiments of the present invention as recited in Claims 1-5, 7, 8, 11, 13, 14, 16, 19-22, 30, 36, 37 and 44 are patentable over the combination of Zhu and Vialen for at least the following rationale.

Applicants respectfully direct the Examiner to independent Claim 1 that recites that an embodiment of the present invention is directed to (emphasis added):

A method for ensuring integrity of data, comprising:
separating an amount of data into segments comprising a plurality of truncatable units, wherein a truncatable unit is a portion of a packet payload that can be truncated from said packet payload;
computing a cryptographic checksum for a said segment;
combining a segment and an associated cryptographic checksum into a data packet; and
applying a header to said data packet, said header comprising information regarding at least one truncation point identifying at least one said truncatable unit of said data packet.

Independent Claims 16 and 30 include similar recitations. Claims 2-5, 7, 8, 11, 13 and 14 that depend from independent Claim 1, Claims 19-22 that depend from independent Claim 16, and Claims 36, 37 and 44 that depend from independent Claim 30 also include these embodiments.

“As reiterated by the Supreme Court in *KSR*, the framework for the objective analysis for determining obviousness under 35 U.S.C. 103 is stated in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966). Obviousness is a question of law based on underlying factual inquiries” including “[a]scertaining the differences between the claimed invention and the prior art” (MPEP 2141(II)). “In determining the differences between the prior art and the claims, the question under 35 U.S.C. 103 is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious”

(emphasis in original; MPEP 2141.02(I)). Applicants note that “[t]he prior art reference (or references when combined) need not teach or suggest all the claim limitations, however, Office personnel must explain why the difference(s) between the prior art and the claimed invention would have been obvious to one of ordinary skill in the art” (emphasis added; MPEP 2141(III)).

Moreover, Applicants respectfully note that “[a] prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention” (emphasis in original; MPEP 2141.02(VI); *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984)).

First, Applicants respectfully submit that Zhu does not teach, describe or suggest “computing a cryptographic checksum for a said segment” and “combining a segment and an associated cryptographic checksum into a data packet” (emphasis added) as recited in independent Claim 1, and the similar recitations of independent Claims 16 and 30.

Applicants respectfully submit that Zhu does not teach, describe or suggest that which it is asserted as teaching, i.e. a cryptographic checksum. With reference to Figure 3 of Zhu, an encryption engine 204 including content-based key generator 302, base layer cipher 304, enhancement layer cipher 314, and stream cipher key 316. Applicants respectfully submit that these

components, alone or in combination, do not teach, describe or suggest the claimed “cryptographic checksum.” In particular, Applicants respectfully submit that the encryption as disclosed in Zhu is used for protection of access to multimedia (see at least [0011] and [0041] through [0048]). However, Applicants respectfully submit that Zhu does not teach, describe or suggest validating the integrity of data, e.g., to verify that the data has not been altered. Accordingly, Applicants respectfully submit that Zhu does not teach, describe or suggest “a cryptographic checksum” as claimed.

Second, Applicants respectfully note the acknowledgement in the Office Action mailed June 19, 2008, that Zhu “does not specifically teach cryptographic checksums” (page 3, line 6). Moreover, the Office Action mailed June 19, 2008, relied on the asserted art “Definition of Cryptographic Checksum” as overcoming this shortcoming. Applicants note that “Definition of Cryptographic Checksum” is not relied on in the instant Office Action. Therefore, by explicitly reciting that Zhu “does not specifically teach cryptographic checksums” in the Office Action mailed June 19, 2008, Applicants respectfully submit that Zhu does not teach, describe or suggest “a cryptographic checksum” as claimed.

Third, Applicants respectfully submit that Zhu does not teach, describe or suggest “applying a header to said data packet, said header comprising information regarding at least one truncation point identifying at least one said

truncatable unit of said data packet" (emphasis added) as recited in independent Claim 1, and the similar recitations of independent Claims 16 and 30.

Applicants understand Zhu to disclose a base layer encrypter that is used for encrypting and authenticating data ([0042]). With reference to FIG. 1 of Zhu, "[t]he exemplary multimedia device 202 receives a scalable multimedia content 102 having a base layer 106 and at least one enhancement layer 108, for example, a scalable MPEG-4 FGS bitstream, and encrypts the multimedia content 102 into a scalable encrypted multimedia content 210 using the exemplary encryption engine 204" ([0036]). In particular, Zhu recites that "[t]he FGS bitstream will be used herein as an example of a scalable multimedia content 102. FGS divides the multimedia content 102 into one base layer 106 and in the following examples, one enhancement layer 108. In the FGS profile, an FGS video object plane mode (FGS VOP) uses the base layer 106 as a reference source for prediction of enhancement layer VOPs while an FGS temporal video object plane mode (FGST VOP) can use forward, backward, or bi-direction prediction from the base layer 106 for enhancement layer VOPs" (emphasis added; [0037]).

With reference to FIG. 3, Zhu recites "[t]he base layer encrypter 104, which receives (and/or derives) the base layer 106 from the multimedia content 102, is communicatively coupled with the enhancement layer encrypter 208,

which receives (and/or derives) one or more enhancement layers 108 from the multimedia content 102” (emphasis added; [0039]). Moreover, with reference to FIG. 2, Zhu recites “[a]s executed by the exemplary encryption engine 204, a sequence of input data, e.g., a segment of a multimedia content 102 representing a video frame or cell of base layer content (that consists of or is analogous to hundreds of "machine words"), is processed by the CBC-type primitive” (emphasis added; [0043]).

Applicants understand Zhu to disclose that the multimedia content 102 is divided into base layer 106 and enhancement layer 108 for separate processing at the encryption engine 204 at base layer encrypter 104 and enhancement layer encrypter 208, respectively (see [0039]). Therefore, Applicants respectfully submit that Zhu does not teach, describe or suggest “applying a header to said data packet, said header comprising information regarding at least one truncation point identifying at least one said truncatable unit of said data packet” (emphasis added) as recited in independent Claim 1, and the similar recitations of independent Claims 16 and 30.

Moreover, Zhu disclose “[a]s shown in FIG. 4, multiple FGST VOPs 402, 404, each with a header 406, 408 may use the same base layer frame 410 as their source of reference VOPs 412” (emphasis added; [0060]). In particular, Applicants respectfully submit that Zhu discloses that each FGST VOP has its

own associated header. Applicants respectfully submit that by disclosing that each FGST VOP has its own header, that Zhu teaches away from “applying a header to said data packet, said header comprising information regarding at least one truncation point identifying at least one said truncatable unit of said data packet” (emphasis added) as recited in independent Claim 1, and the similar recitations of independent Claims 16 and 30.

Fourth, Applicants respectfully submit that Vialen does not overcome the shortcomings of Zhu. In particular, Applicants respectfully submit that Vialen also does not teach, describe or suggest “computing a cryptographic checksum for a said segment” and “combining a segment and an associated cryptographic checksum into a data packet” (emphasis added) as recited in independent Claim 1, and the similar recitations of independent Claims 16 and 30. Applicants understand Vialen to disclose an adaptive message authentication code. In particular, Applicants respectfully submit that Vialen is silent to a “cryptographic checksum” as claimed.

Moreover, Applicants respectfully submit that Vialen also does not teach, describe or suggest “applying a header to said data packet, said header comprising information regarding at least one truncation point identifying at least one said truncatable unit of said data packet” (emphasis added) as recited in

independent Claim 1, and the similar recitations of independent Claims 16 and 30.

As presented above, Applicants understand Vialen to disclose an adaptive message authentication code. Applicants respectfully submit that Vialen disclose that “[i]f the length of the message is shorter than the length of the block size, then the computed message authentication code is truncated to fit in the remaining space” (emphasis added; Abstract). Applicants respectfully submit that Vialen does not teach, describe or suggest a “truncation point” as claimed. In particular, Applicants submit that Vialen is silent to such a teaching. Therefore, Applicants respectfully submit that Vialen also does not teach, describe or suggest “applying a header to said data packet, said header comprising information regarding at least one truncation point identifying at least one said truncatable unit of said data packet” (emphasis added) as recited in independent Claim 1, and the similar recitations of independent Claims 16 and 30.

Therefore, Applicants respectfully submit that Vialen shares at least some of the shortcomings of Zhu. Thus, Vialen, alone or in combination with Zhu, does not show or suggest the embodiments as claimed.

Applicants respectfully assert that the combination of Zhu and Vialen does not teach, disclose or suggest the claimed embodiments of the present invention as recited in independent Claims 1, 16 and 30, that these claims overcome the rejection under 35 U.S.C. § 103(a), and that these claims are thus in a condition for allowance. Therefore, Applicants respectfully submit that the combination of Zhu and Vialen also does not teach or suggest the additional claimed features of the present invention as recited in Claims 2-5, 7, 8, 11, 13 and 14 that depend from independent Claim 1, Claims 19-22 that depend from independent Claim 16, and Claims 36, 37 and 44 that depend from independent Claim 30. Therefore, Applicants respectfully submit that Claims 2-5, 7, 8, 11-14, 19-22, 36, 37 and 44 also overcome the rejection under 35 U.S.C. § 103(a), and are in a condition for allowance as being dependent on an allowable base claim.

35 U.S.C. §103(a) - 6, 9, 10, 15, 17, 18, 23-29, 31-35 and 38-43

The instant Office Action asserts that Claims 6, 9, 10, 15, 17, 18, 23-29, 31-35 and 38-43 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Zhu in view of Vialen, further in view of U.S. Patent No. 6,963,972 by Chang et al., hereinafter referred to as the “Chang” reference. Claim 6 is cancelled herein without prejudice; therefore a discussion of the rejection of Claim 6 is moot at this time. Applicants have reviewed Zhu, Vialen and Chang, and respectfully submit that the embodiments of the present invention as recited in Claims 9, 10, 15, 17, 18, 23-29, 31-35 and 38-43 are patentable over the combination of Zhu, Vialen and Chang for at least the following rationale.

Claims 9, 10 and 15 are dependent on independent Claim 1 and include the recitations of Claim 1, Claims 17, 18 and 23-29 are dependent on independent Claim 16 and include the recitations of Claim 16, and Claims 31-35 and 38-43 are dependent on independent Claim 30 and include the recitations of Claim 30. Hence, by demonstrating that Zhu, Vialen and Chang do not show or suggest the embodiments of Claims 1, 16 and 30, it is also demonstrated that Zhu, Vialen and Chang do not show or suggest the embodiments of Claims 6, 9, 10, 15, 17, 18, 23-29, 31-35 and 38-43.

As described above, Applicants respectfully submit that the combination of Zhu and Vialen does not teach, describe or suggest “computing a cryptographic checksum for a said segment,” “combining a segment and an associated cryptographic checksum into a data packet” and “applying a header to said data packet, said header comprising information regarding at least one truncation point identifying at least one said truncatable unit of said data packet” (emphasis added) as claimed.

Further, Applicants respectfully submit that the combination of Zhu, Vialen and Chang fails to teach or suggest this claim limitation because Chang does not overcome the shortcomings of Zhu and Vialen. Applicants understand Chang to disclose a method and apparatus for networked information dissemination through secure transcoding (Title). In particular, Applicants respectfully submit

that Chang also does not teach, describe or suggest “computing a cryptographic checksum for a said segment” and “combining a segment and an associated cryptographic checksum into a data packet” (emphasis added) as recited in independent Claim 1, and the similar recitations of independent Claims 16 and 30. In particular, Applicants respectfully submit that Chang is silent to a “cryptographic checksum” as claimed.

Moreover, Applicants respectfully submit that Chang also does not teach, describe or suggest “applying a header to said data packet, said header comprising information regarding at least one truncation point identifying at least one said truncatable unit of said data packet” (emphasis added) as recited in independent Claim 1, and the similar recitations of independent Claims 16 and 30.

Applicants respectfully submit that Chang does not teach, describe or suggest a “truncation point” as claimed. In particular, Applicants submit that Chang is silent to such a teaching. Therefore, Applicants respectfully submit that Chang also does not teach, describe or suggest “applying a header to said data packet, said header comprising information regarding at least one truncation point identifying at least one said truncatable unit of said data packet” (emphasis added) as recited in independent Claim 1, and the similar recitations of independent Claims 16 and 30.

Therefore, Applicants respectfully submit that Chang shares at least some of the shortcomings of Zhu and Vialen. Thus, Zhu, Vialen and Chang, alone or in combination, do not show or suggest the embodiments as claimed.

Applicants respectfully assert that the combination of Zhu, Vialen and Chang does not teach, disclose or suggest the claimed embodiments of the present invention as recited in independent Claims 1, 16 and 30, that these claims overcome the rejection under 35 U.S.C. § 103(a), and that these claims are thus in a condition for allowance. Applicants respectfully submit that the combination of Zhu, Vialen and Chang also does not teach or suggest the additional claimed features of the present invention as recited in Claims 9, 10 and 15 that depend from independent Claim 1, Claims 17, 18 and 23-29 that depend from independent Claim 16, and Claims 31-35 and 38-43 that depend from independent Claim 30. Therefore, Applicants respectfully submit that Claims 9, 10, 15, 17, 18, 23-29, 31-35 and 38-43 also overcome the rejection under 35 U.S.C. § 103(a), and are in a condition for allowance as being dependent on an allowable base claim.

CONCLUSION

Based on the arguments presented above, Applicants respectfully assert that Claims 1-5, 7-11, 13-16 and 18-44 overcome the rejections of record and, therefore, Applicants respectfully solicit allowance of these Claims.

Respectfully submitted,

WAGNER BLECHER L.L.P.

Dated: March 18, 2009

/John P. Wagner, Jr./

John P. Wagner, Jr.
Registration No. 35,398

Address:

WAGNER BLECHER LLP
Westridge Business Park
123 Westridge Drive
Watsonville, California 95076
(408) 377-0500